IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:15-CR-322
	)	
Plaintiff,	)	JUDGE DAN AARON POLSTER
	)	
v.	)	
	)	GOVERNMENT'S MEMORANDUM IN
JOHN CLEMENTS,	)	OPPOSITION TO DEFENDANT'S
	)	MOTION TO COMPEL DISCOVERY
Defendant.	)	

Now comes the United States of America, by and through counsel, Steven M. Dettelbach, United States Attorney, and Brian M. McDonough, Assistant U. S. Attorney, and respectfully requests that the Court deny defendant John Clements' motion to compel discovery of the proprietary, non-public, sensitive software because the software is not in the possession custody or control of the government, the software is not material to Clements' defense, and for the reasons stated in the attached memorandum.

Respectfully submitted,

STEVEN M. DETTELBACH
United States Attorney

By: /s/ Brian McDonough
Brian McDonough (OH: 0072954)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3965
(216) 522-2403 (facsimile)
Brian.McDonough@usdoj.gov

MEMORANDUM

I. INTRODUCTION

Defendant John Clements has moved to compel discovery of the software known as Child Protection System (CPS) including the Shareaza LE software program, as well as all documents and records in the Government's possession, custody and control regarding the investigation of this case. (R. 17, Motion to Compel, PageID 70).

Prior to the motion's filing, the government complied with Rule 16 of the Federal Rules of Criminal Procedure and provided Clements with the discovery required under Criminal Rule 16, including the logs and reports produced by the investigator during this investigation. Although the Government provided Clements with Rule 16 documents and records, Clements not seeks the software programs. The Government submits the following Memorandum in Opposition to Defendant's Motion to Compel Discovery and respectfully urges this Court to deny the motion.

II. STATEMENT OF FACTS

A. The investigation and offense conduct

In February 2014, Donald Seamon, a Lake County deputy sheriff's detective with the Federal Bureau of Investigation Child Exploitation Task Force was conducting began an investigation of an individual sharing child pornography on the Gnutella 2 peer-to-peer network. Seamon described, in detail, his investigation in a search warrant affidavit in this matter. (R. 17-1, Affidavit, PageID 71-72). Seamon described how a peer-to-peer network works and how his law enforcement software interfaced with the network. (Id., PageID 72). Seamon described how he noticed a computer sharing child pornography from a specific IP address, subscribed to by Clements in Lake County, Ohio. (Id., PageID 74). Seamon further noted that he established a direct connection with the computer in question and downloaded four complete files and three partial files of child pornography on May 5, 2014. (Id., PageID 72-73).

B. The software

The software at issue here consist of a peer-to-peer program, ShareazaLE and a database maintained as part of the CPS. CPS is a suite of programs, owned by a private company, TLO, and used exclusively by law enforcement. (Exhibit A, paragraph 2). As law enforcement officers, licensed to use CPS, use the software applications, their work is logged to the CPS database. (Id., paragraph 3). In this way, law enforcement officers around the world can pool their efforts and help identify targets who are operating on the global Internet. The software application, used by Seamon in this case, was ShareazaLE, a product of TLO. ShareazaLE is a version of Shareaza, an open-source peer-to-peer filing sharing software. Programmers at TLO modified it to assist in law enforcement efforts. Most peer-to-peer software downloads files from multiple sources to expedite the download and balance the load on the network. ShareazaLE was modified to ensure that the files are downloaded exclusively from the target computer. (Exhibit A, paragraph 7). ShareazaLE is not capable of placing data on a target computer or from retrieving data from a target computer, other than the data made publically available by that user.

III. LAW AND ARGUMENT

A. Proprietary, non-public and sensitive surveillance software is protected by qualified privilege and should not be discovered.

As an initial matter, Clements should not be allowed access to proprietary, non-public and sensitive investigatory technology such as ShareazaLE, the program used in this case, absent a showing of particular need. At least three Circuits have found that disclosure of such investigatory methods is protected by a qualified privilege in a variety of contexts and have required that defendants overcome this in order to compel discovery. United States v. Green, 670 F.2d 1148, 1155 (D.C. Cir. 1981) (in suppression hearing, recognizing qualified privilege for surveillance locations and balancing test to overcome it); United States v. Cintolo, 818 F.2d 980, 1001-02 (1st Cir. 1987) (limiting cross-examination re: surveillance locations); United States v. Harley, 682 F.2d 1018, 1020 (D.C. Cir. 1982) (holding defendant "should ordinarily show that he needs the evidence to conduct his defense and that there are no adequate alternative means of getting at the same point" when seeking testimony about sensitive information on cross-examination); United States v. Van Horn, 789 F.2d 1492, 1508 (11th Cir. 1986) (affirming denial of discovery requests for electronic surveillance locations); see also In re Dep't of Investigation of the City of New York, 856 F.2d 481 (2d Cir. 1988) (recognizing law enforcement privilege against Rule 17 subpoena of investigatory files).

The First Circuit Court of Appeals in United States v. Chiaradio, 684 F.3d 265, 278 (2012), recently considered this qualified privilege, which it had recognized in Cintolo, 818 F.2d at 1002, as it applied to a motion to compel discovery of the source code for EP2P, a similar law enforcement program used by the FBI. While the court in Chiaradio did not have to base its denial of the motion on this privilege, the court strongly implied that the privilege would operate to bar discovery in such a case "because the government reasonably fears that traders of child pornography (a notoriously computer-literate group) otherwise would be able to use the source code to develop ways either to evade apprehension or to mislead the authorities." Chiaradio, 684 F.3d at 278. This is precisely the concern expressed by the Eleventh Circuit in Van Horn, that "[d]isclosing the precise locations where surveillance devices are hidden or their precise specifications will educate criminals regarding how to protect themselves against police surveillance." 789 F.2d at 1508. In United States v. Budziak, 697 F.3d 1105, 1111-13 (9th Cir.

2012), the Ninth Circuit held that the government should have disclosed the EP2P software. While the government submits that case was wrongly decided, the affidavit of the Defense expert, in Budziak, seemingly had more detail, calling into question the quality of the government's evidence which the court found justified further discovery.

Here, ShareazaLE is a part of a suite of law enforcement software programs known as Child Protection Systems (CPS) that is developed and managed by a private company called TLO, Inc. (TLO). TLO licenses law enforcement personnel worldwide to use CPS in order to detect the distribution of child pornography in their respective jurisdictions. Only trained and licensed users who are actively involved in the investigation of child exploitation are allowed access to the system. As outlined in a prior affidavit of William S. Wiltse, attached hereto as Exhibit A, certain highly sensitive information would be compromised by allowing a defense expert access to copy of ShareazaLE or CPS. As detailed by Wiltse, every user of the software is a specifically trained law enforcement officer, and during the officer's use of the software, data is automatically logged to the CPS server. (Exhibit A, paragraph 3). This ensures that the data contained in the CPS database is the product of the CPS software and law enforcement efforts.

To allow a defense expert access to the software would destroy the integrity of the database, as the expert's use of the software would be logged to the database, and investigators around the world would no longer be able to assure courts that the data was the exclusive product of the CPS software and law enforcement. Additionally, giving a defense expert access to the software would be giving him access to a database full of information about people currently sharing child pornography. This could negatively effect current investigations and put law enforcement officers at risk.

Because the computer program employed here is a sensitive, non-public investigatory method, the Government urges this court to find a qualified privilege against discovery of ShareazaLE and CPS and to deny Clements' motion to compel for lack of a showing of a sufficiently compelling need. See Van Horn, 789 F.2d at 1508 (holding claim "that the information was necessary to demonstrate that the voices on the tapes could have been distorted, resulting in improper voice identifications" insufficient to overcome privilege). Clements has not established, for example, why cross-examination of the Government's witnesses on issues such as the reliability of ShareazaLE and CPS is insufficient to get at the same point absent discovery of a copy of the software.

Further, as argued below, the Government is not in possession of the source code that would be necessary for Clements or an independent expert to effectively test the reliability of ShareazaLE and CPS; the copy of the software that the Government could provide would be of no help to Clements on this issue and thus it would be unreasonable for this Court to compel its production.

B. Clements is not entitled to discovery of software used in this case because he has not shown materiality and the reasonableness of his requests.

Clements argues that Rule 16 of the Federal Rules of Criminal Procedure entitles him to discovery of the software known as CPS including the Shareaza LE software program for this case. (R. 17, Motion to Compel, PageID 70).

The Government has previously turned over all relevant records to Clements including the summary reports and logs of ShareazaLE, the computer program Seamon used to connect to Clements' computer, identify and download shared files containing child pornography, and identify IP address associated with it at various times.

Clements claims primarily that this Court should compel the Government to provide the requested discovery under Federal Criminal Rule 16(a)(1)(E)(i) because they are material to preparing the defense. "[T]he requirement of [Rule 16(a)(1)(E)(i)] of a showing of the reasonableness and materiality of the request is not satisfied by a mere conclusory allegation that the requested information is material to the preparation of the defense." United States v. Conder, 423 F.2d 904, 910 (6th Cir. 1970) (citations omitted). This Court should deny Clements' motion because he has failed to show that the items requested are material to his case and because his request for access to sensitive, non-public law enforcement software is not reasonable under the circumstances.

Clements first contention appears to be that his expert wishes to know whether the law enforcement officer went beyond the scope of publicly available information on his computer and that this Court should compel discovery to allow him to explore. (R. 17, Motion to Compel, PageID 79). However, the software used by law enforcement to search peer-to-peer networks in this case has no capacity to manipulate data or alter sharing settings on a target computer. (Exhibit A, paragraph 8). The Government would be willing to present expert testimony at an evidentiary hearing to this effect if this Court so orders. In any case, this Court should not compel discovery of sensitive law enforcement investigation tools based on Clements' expert's unfounded hunch that law enforcement officers may have manipulated data on Clements' computer.

Second, Clements appears to be concerned with the software's "reliability and accuracy" (R. 17, Motion to Compel, PageID 80), but discovery of the specific law enforcement programs and methods used here is completely unnecessary for that purpose. Error is practically non-existent in the ShareazaLE and CPS systems, just as in Chiaradio, 684 F.3d at 278, where the government's expert testified that "the program, with respect to identifying the source of particular files, had no error rate." The Government is also willing to offer expert testimony at an evidentiary hearing as to the error rate involved if this Court so orders. The government has provided Clements with the logs created when Seamon connected to Clements' computer and downloaded files. These logs demonstrate the activity between the computers. Having access to the actual law enforcement software would add nothing to an error analysis. It would be unreasonable to turn over and likely compromise the security of a sensitive law enforcement tool to confirm a likely non-existent error rate.

Lastly, Clements' arguments for production focus largely on issues of testing the reliability of ShareazaLE and CPS and the leads produced through them. Wiltse has confirmed, however, that Defendant will not be able to determine anything about the reliability of ShareazaLE or how it operates without access to the source code for the program. (Exhibit A, paragraph 10). The ShareazaLE source code was the property of TLO, Inc. and is not in the Government's possession or otherwise accessible to the Government. (Id., paragraphs 10-12). A simple copy of the ShareazaLE software would therefore not be material to Clements' case on the grounds of testing the program's reliability. The Government cannot produce in discovery what it does not have. Similarly, the Government cannot provide details about any records, logs or reports created and stored on the CPS, (other than those produced by Seamon during this investigation - which have been provided to Clements) servers because it does not have direct access to them.

IV. CONCLUSION

For the foregoing reasons, the Government respectfully requests that this Court deny Clements' motion to compel discovery.

CERTIFICATE OF SERVICE

I hereby certify that on this 26th day of January 2016 a copy of the foregoing document was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. All other parties will be served by regular U.S. Mail. Parties may access this filing through the Court's system.

/s/ Brian McDonough
Brian McDonough
Assistant U.S. Attorney